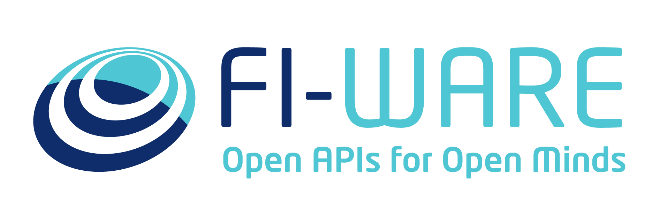
**MNCA IOT SmartCity Technical Architecture**

****

****

**DSI Métropole Nice Côte d’Azur**

**IOT & Smart City Platform**

|  |  |
| --- | --- |
| VERSION: draft | REVISION DATE: 02/11/2017 |

Approval of the Technical Architecture indicates an understanding of the purpose and content described in this deliverable. By signing this deliverable, each individual agrees with the content contained in this deliverable.

|  |  |  |  |
| --- | --- | --- | --- |
| **Approver Name** | **Title** | **Signature** | **Date** |
| Stéphane Roux | ICT Quality Assurance Engineer |  |  |
| Lionel Chaudanson | Responsable technique, IOT & Smart City |  |  |
| Serge Massiera | Directeur des Systèmes d'Information |  |  |
|  |  |  |  |
|  |  |  |  |

[1 Section 1 DOCUMENT SCOPE 6](#_Toc497400317)

[1.1 Context 6](#_Toc497400318)

[1.2 Glossary 8](#_Toc497400319)

[2 Section 2 OVERALL TECHNICAL ARCHITECTURE 9](#_Toc497400320)

[2.1 System Architecture Context Diagram 9](#_Toc497400321)

[2.2 System Architecture Model 11](#_Toc497400322)

[2.2.1 Overall Architectural Considerations 12](#_Toc497400323)

[2.3 System Architecture Component Definitions 15](#_Toc497400328)

[2.3.1 Security Component IDM GE 15](#_Toc497400329)

[2.3.2 Orion Context Broker Component 15](#_Toc497400331)

[2.3.3 MongoDB Component 15](#_Toc497400332)

[2.3.4 Citus/PostgreSQL Cluster Component 15](#_Toc497400333)

[2.3.5 Galera/MySQL Cluster Component 15](#_Toc497400334)

[2.3.6 Cosmos Big Data Component 15](#_Toc497400335)

[2.3.7 Knowage Analytics Component 16](#_Toc497400336)

[2.3.8 CKAN Open Data Component 16](#_Toc497400337)

[2.3.9 IDAS Component 16](#_Toc497400338)

[2.3.10 CEP Component 17](#_Toc497400339)

[2.3.11 Application Mashup Component 17](#_Toc497400340)

[2.3.12 Biz Ecosystem Component 17](#_Toc497400341)

[2.3.13 Development Components 18](#_Toc497400342)

[2.3.14 Monitoring Components 18](#_Toc497400343)

[2.3.15 Docker Images Management Component 18](#_Toc497400344)

[2.3.16 Docker Swarm Management Component 18](#_Toc497400345)

[3 Section 3 SYSTEM ARCHITECTURE DESIGN 18](#_Toc497400346)

[3.1 Security Component IDM GE 18](#_Toc497400347)

[3.1.1 Component Functions 18](#_Toc497400348)

[3.1.2 Technical Considerations 19](#_Toc497400349)

[3.1.3 Selected Product(s) 19](#_Toc497400350)

[3.1.4 Selection Rationale 19](#_Toc497400351)

[3.1.5 Architecture Risks 19](#_Toc497400352)

[3.2 Orion Context Broker Component 19](#_Toc497400353)

[3.2.1 Component Functions 19](#_Toc497400354)

[3.2.2 Technical Considerations 19](#_Toc497400355)

[3.2.3 Selected Product(s) 19](#_Toc497400356)

[3.2.4 Selection Rationale 19](#_Toc497400357)

[3.2.5 Architecture Risks 19](#_Toc497400358)

[3.3 MongoDB Component 19](#_Toc497400359)

[3.3.1 Component Functions 19](#_Toc497400360)

[3.3.2 Technical Considerations 19](#_Toc497400361)

[3.3.3 Selected Product(s) 19](#_Toc497400362)

[3.3.4 Selection Rationale 19](#_Toc497400363)

[3.3.5 Architecture Risks 19](#_Toc497400364)

[3.4 Citus/PostgreSQL cluster Component 20](#_Toc497400365)

[3.4.1 Component Functions 20](#_Toc497400366)

[3.4.2 Technical Considerations 20](#_Toc497400367)

[3.4.3 Selected Product(s) 20](#_Toc497400368)

[3.4.4 Selection Rationale 20](#_Toc497400369)

[3.4.5 Architecture Risks 20](#_Toc497400370)

[3.5 Galera/MySQL cluster Component 20](#_Toc497400371)

[3.5.1 Component Functions 20](#_Toc497400372)

[3.5.2 Technical Considerations 20](#_Toc497400373)

[3.5.3 Selected Product(s) 20](#_Toc497400374)

[3.5.4 Selection Rationale 20](#_Toc497400375)

[3.5.5 Architecture Risks 20](#_Toc497400376)

[3.6 Cosmos Big Data Component 20](#_Toc497400377)

[3.6.1 Component Functions 20](#_Toc497400378)

[3.6.2 Technical Considerations 20](#_Toc497400379)

[3.6.3 Selected Product(s) 20](#_Toc497400380)

[3.6.4 Selection Rationale 20](#_Toc497400381)

[3.6.5 Architecture Risks 20](#_Toc497400382)

[3.7 Knowage Analytics Component 20](#_Toc497400383)

[3.7.1 Component Functions 20](#_Toc497400384)

[3.7.2 Technical Considerations 20](#_Toc497400385)

[3.7.3 Selected Product(s) 20](#_Toc497400386)

[3.7.4 Selection Rationale 20](#_Toc497400387)

[3.7.5 Architecture Risks 20](#_Toc497400388)

[3.8 CKAN Open Data Component 21](#_Toc497400389)

[3.8.1 Component Functions 21](#_Toc497400390)

[3.8.2 Technical Considerations 21](#_Toc497400391)

[3.8.3 Selected Product(s) 21](#_Toc497400392)

[3.8.4 Selection Rationale 21](#_Toc497400393)

[3.8.5 Architecture Risks 21](#_Toc497400394)

[3.9 IDAS Component 21](#_Toc497400395)

[3.9.1 Component Functions 21](#_Toc497400396)

[3.9.2 Technical Considerations 21](#_Toc497400397)

[3.9.3 Selected Product(s) 21](#_Toc497400398)

[3.9.4 Selection Rationale 21](#_Toc497400399)

[3.9.5 Architecture Risks 21](#_Toc497400400)

[3.10 CEP Component 21](#_Toc497400401)

[3.10.1 Component Functions 21](#_Toc497400402)

[3.10.2 Technical Considerations 21](#_Toc497400403)

[3.10.3 Selected Product(s) 21](#_Toc497400404)

[3.10.4 Selection Rationale 21](#_Toc497400405)

[3.10.5 Architecture Risks 21](#_Toc497400406)

[3.11 Application Mashup Component 21](#_Toc497400407)

[3.11.1 Component Functions 21](#_Toc497400408)

[3.11.2 Technical Considerations 21](#_Toc497400409)

[3.11.3 Selected Product(s) 21](#_Toc497400410)

[3.11.4 Selection Rationale 21](#_Toc497400411)

[3.11.5 Architecture Risks 21](#_Toc497400412)

[3.12 Biz Ecosystem Component 22](#_Toc497400413)

[3.12.1 Component Functions 22](#_Toc497400414)

[3.12.2 Technical Considerations 22](#_Toc497400415)

[3.12.3 Selected Product(s) 22](#_Toc497400416)

[3.12.4 Selection Rationale 22](#_Toc497400417)

[3.12.5 Architecture Risks 22](#_Toc497400418)

[3.13 Development Components 22](#_Toc497400419)

[3.13.1 Component Functions 22](#_Toc497400420)

[3.13.2 Technical Considerations 22](#_Toc497400421)

[3.13.3 Selected Product(s) 22](#_Toc497400422)

[3.13.4 Selection Rationale 22](#_Toc497400423)

[3.13.5 Architecture Risks 22](#_Toc497400424)

[3.14 Monitoring Components 22](#_Toc497400425)

[3.14.1 Component Functions 22](#_Toc497400426)

[3.14.2 Technical Considerations 22](#_Toc497400427)

[3.14.3 Selected Product(s) 22](#_Toc497400428)

[3.14.4 Selection Rationale 22](#_Toc497400429)

[3.14.5 Architecture Risks 22](#_Toc497400430)

[3.15 Docker Images Management Component 22](#_Toc497400431)

[3.15.1 Component Functions 22](#_Toc497400432)

[3.15.2 Technical Considerations 22](#_Toc497400433)

[3.15.3 Selected Product(s) 22](#_Toc497400434)

[3.15.4 Selection Rationale 22](#_Toc497400435)

[3.15.5 Architecture Risks 22](#_Toc497400436)

[3.16 Docker Swarm manager Component 23](#_Toc497400437)

[3.16.1 Component Functions 23](#_Toc497400438)

[3.16.2 Technical Considerations 23](#_Toc497400439)

[3.16.3 Selected Product(s) 23](#_Toc497400440)

[3.16.4 Selection Rationale 23](#_Toc497400441)

[3.16.5 Architecture Risks 23](#_Toc497400442)

[4 Section 4 System Construction Environment 23](#_Toc497400443)

[4.1 Development Environment 23](#_Toc497400444)

[4.1.1 Developer Workstation Configuration 23](#_Toc497400445)

[4.1.2 Supporting Development Infrastructure Configuration 23](#_Toc497400446)

[4.2 QA Environment 23](#_Toc497400447)

[4.2.1 QA Workstation Configuration 23](#_Toc497400448)

[4.2.2 Supporting QA Infrastructure Configuration 23](#_Toc497400449)

[4.3 Acceptance Environment 23](#_Toc497400450)

[4.3.1 Acceptance Workstation Configuration 23](#_Toc497400451)

[4.3.2 Supporting Acceptance Infrastructure Configuration 23](#_Toc497400452)

# Section 1 DOCUMENT SCOPE

## Context

***Document Scope*** *describes the context and the goals of this document in a narrative.*

This document describes the Technical Architecture of the IOT Smart City Platform that:

* satisfies business requirements as documented in the roadmap (ref to provide),
* satisfies technical, operational and transitional requirements.

The goal of this Technical Architecture is to define the technologies, products, and techniques necessary to install and support the system, and to ensure that the system components are compatible and comply with the enterprise-wide standards and direction defined by Nice Côte d’Azur metropolis (hereafter referred as MNCA).

This document will also:

* Identify and explain the risks inherent in this Technical Architecture;
* Define baseline sizing, archiving and performance requirements;
* Identify the hardware and software specifications for the Development, Testing, QA and Production environments;
* Identify monitoring and support tools for maintenance in operational condition
* Define procedures for data migration among the environments (current datawarehouse).

The MNCA IOT Smart City Platform will be deployed upon the 3 data centers owned and managed by the MNCA DSI

* The main data center is Phoenix,
* The secondary is Bosio (currently underworks for revamping for 6 months),
* The third one (the smallest) is Biscarra, (the configuration has to be reconsidered but after Bosio .
* The hardware infrastructure is based on bare metal servers (Cisco and a few remaining HP)
* The servers are blades in enclosures, 3 enclosures per cabinet
* The machines are managed with VMWare ESX as virtualization layer, vCenter, vMotion.
* There is a redundant SAN (EMC), dispatched in main and secondary DC.
* It exists also a redundant NAS system for low I/O file storage.

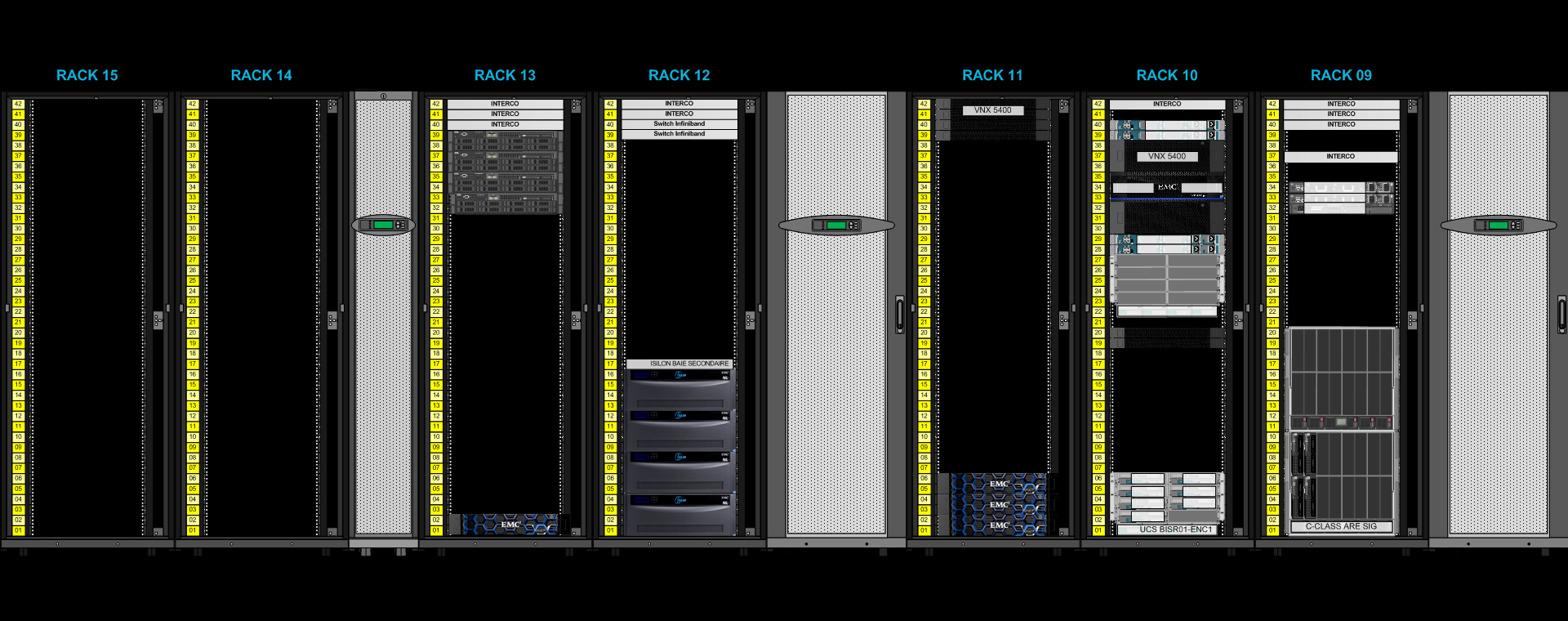
MNCA Network is managed with a cluster of firewall/routers, managing the separation in 4 different virtual networks

* Public DMZ for applications
* Private DMZ
* LAN
* Field LAN for IOT gateways, devices and sensors

There’s several Load balancing F5 Big IP appliances at strategic points to distribute load to data centres.

On next page is presented the overview of the Phoenix main Data Centre.







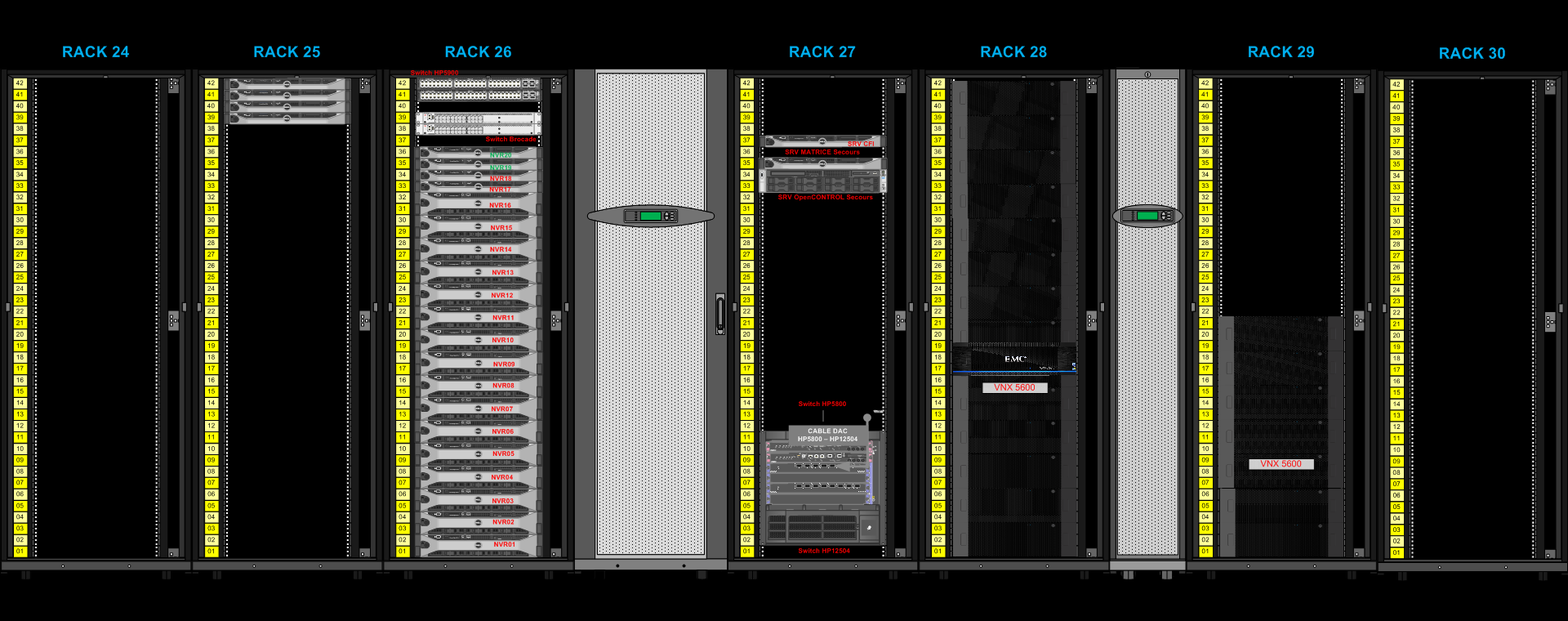


Figure 1: Poenix DC overview

## Glossary

**FIWARE**: is an independent open community whose members are committed to materialize the FIWARE mission, that is: “to build an open sustainable ecosystem around public, royalty-free and implementation-driven software platform standards that will ease the development of new Smart Applications in multiple sectors”.

**Fiware platform**: is a platform providing a simple but powerful set of APIs that ease the development of Smart Applications in multiple vertical sectors: <https://www.fiware.org/>

**IOT**: Internet Of Things

**OMA**: [Open Mobile Alliance](http://www.openmobilealliance.org/) : OMA is a non-profit organization that delivers open specifications for creating interoperable services that work across all geographical boundaries, on any bearer network.

**TM Forum**: is the global industry association that drives digital transformation of the communications industry through collaboration.

**GE**: Generic Enabler, Fiware used terminology to design an essential module of the platform

**API**: Application Programming Interface

**Context Broker**: According to Gartner:

“A context broker is a service that is designed to gather reachable context data of a variety of types, sources and velocity. It then applies conditioning, integration, rules and analytics to derive the reduced prepared context data, actionable at a point of business decision by a system or a human.”

Functionally speaking, context enables the data to be empowered by the interaction with other pieces of data. In a nutshell it can be consider as a data exchange bus, providing publish/subscribe of context information.

**NGSI**: New Generation Services Interface, [OMA referenced API specifications](http://www.openmobilealliance.org/release/NGSI/) defined ([NGSI V9 and V10](https://forge.fiware.org/plugins/mediawiki/wiki/fiware/index.php/NGSI-9/NGSI-10_information_model)) and used with amendments by Fiware (Context Broker) as the dorsal for the platform

**Docker**: is a virtualization software technology providing containers to run software applications in isolation:

**Swarm**: Docker Swarm provides native clustering functionality for Docker containers, which turns a group of Docker engines into a single, virtual Docker engine.

**VRF**: Virtual Routing and Forwarding network component.

**GDPR**: General Data Protection Regulation

**RIA**: Rich Internet Application

# Section 2 OVERALL TECHNICAL ARCHITECTURE

## 2.1 System Architecture Context Diagram

The **Smart city plarform Architecture Context Diagram** provides the “big picture” view of the global system’s architecture, and puts it in context with the rest of the Performing Organization’s systems portfolio, illustrating how the system’s hardware and software platforms fit into the existing environment.



Figure 2: MNCA Infrastructure Global View

The above schema shows globally the IT and network infrastructure in place for MNCA.

Since servers are dispatched through the 4 VLANs independently from the cabinets, the schema is not the true image of cabinets repartition in the different VLANs

The existing IT services for MNCA are deployed through this available infrastructure.

The Smart city platform will as well be deployed on the same data center infrastructure, but a new DMZ network

Nevertheless, it might be that some new hardware will be required (servers, router/firewall, Load balancer)

The envisaged interaction between those services and the smart City platform is for the moment limited to:

* use MNCA mail services (outgoing/incoming)
* connect existing data sources to the new system instead of the current used data warehouse
* potentially use global MNCA security system based on Microsoft Adam (LDAP server), if necessary

The MNCA smart city platform wil be based on [FIWARE](https://www.fiware.org/)

The Fiware community propose a set of modules called Generic Enablers, which provide the essential software bricks to set a complete smart city platform, like a kind of “Lego”.

The most important to mention is that FIWARE has deliberately chosen to go towards a container based architecture, this remove the dependency with Openstack initially thought as the preferred cloud stack for deploying Fiware platforms.

Fiware started in 2014, which was just the beginning of the “Dockerization” of the server software world, the Fiware consortium couldn’t stay without going towards container based deployment, Docker is now an officially supported way to deploy Fiware components in a very clear and easy way.

MNCA have the opportunity to introduce new way to use its infrastructure using container based architecture, by choosing to use Docker to deploy its own Fiware plarform as a reference Smart City Platform.

The global architecture of the MNCA Fiware platform will rely on a Docker Swarm composed of nodes dispatched in the different VLANs.

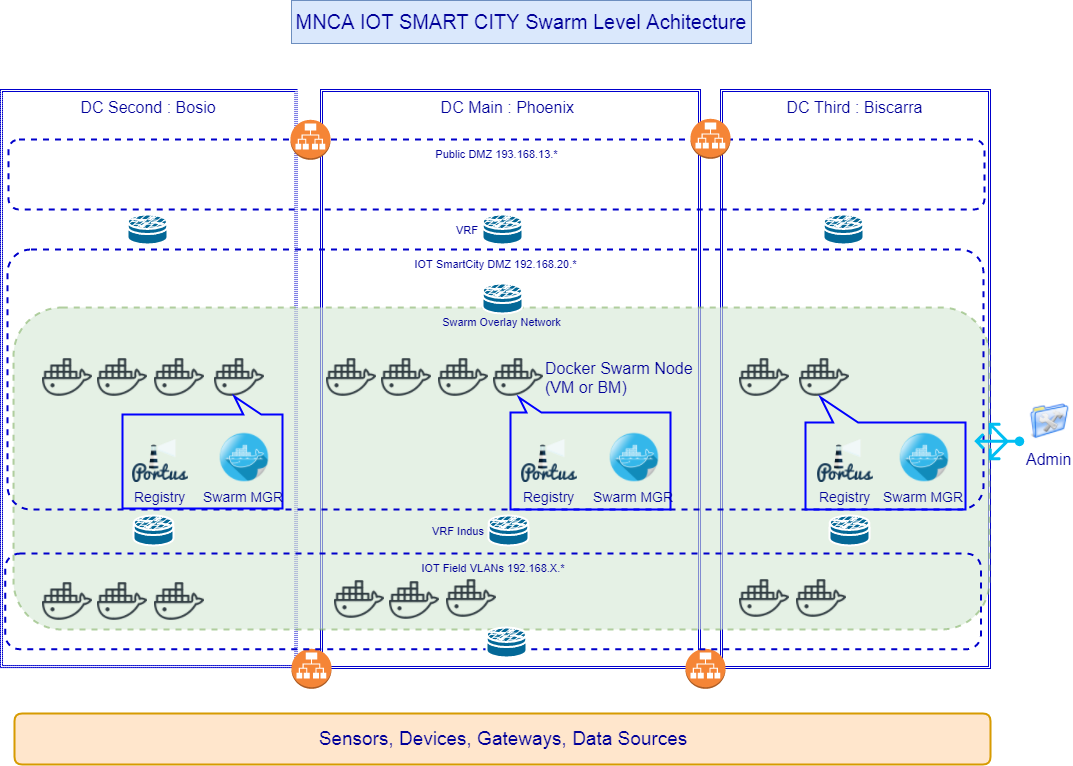


Figure 3: Docker swarm deployment for MNCA Smart city Fiware platform

A Docker swarm solution has been chosen in a first step because of the ease of use and configuration.

The learning curve of Docker container orchestration tool: Swarm, is less sloppy than other solution like Kubernetes (the open source declination of the Google internal orchestration tool: Borg), which sit at the top in term of features, openness, and adoption, among cloud orchestration tools today’s landscape.

It is the right choice to start with simple Docker Swarm, anyway it will be easy to add later another orchestration tool like Kubernetes, since it will be proposed as the Swarm complement in Docker Enterprise distribution ([very recent news](https://thenewstack.io/docker-fully-embraces-kubernetes/)).

Then the MNCA FIWARE smart city platform will be deployed in a global docker swarm covering the 3 data centers.

The repartition of the traffic between the data centers will be managed by F5 BigIP load balancing appliance.

However to minimize configuration task on load balancer (limit to load repartition between data centers of main categories of services), for the lower granularity of applications, and internal components of the platform, simple load balancing and fail-over mechanisms are managed automatically by the Docker Swarm (number of instances of a service).

## System Architecture Model

The **System Architecture Model** represents the various architecture components that comprise the system, and shows the important interrelationships.

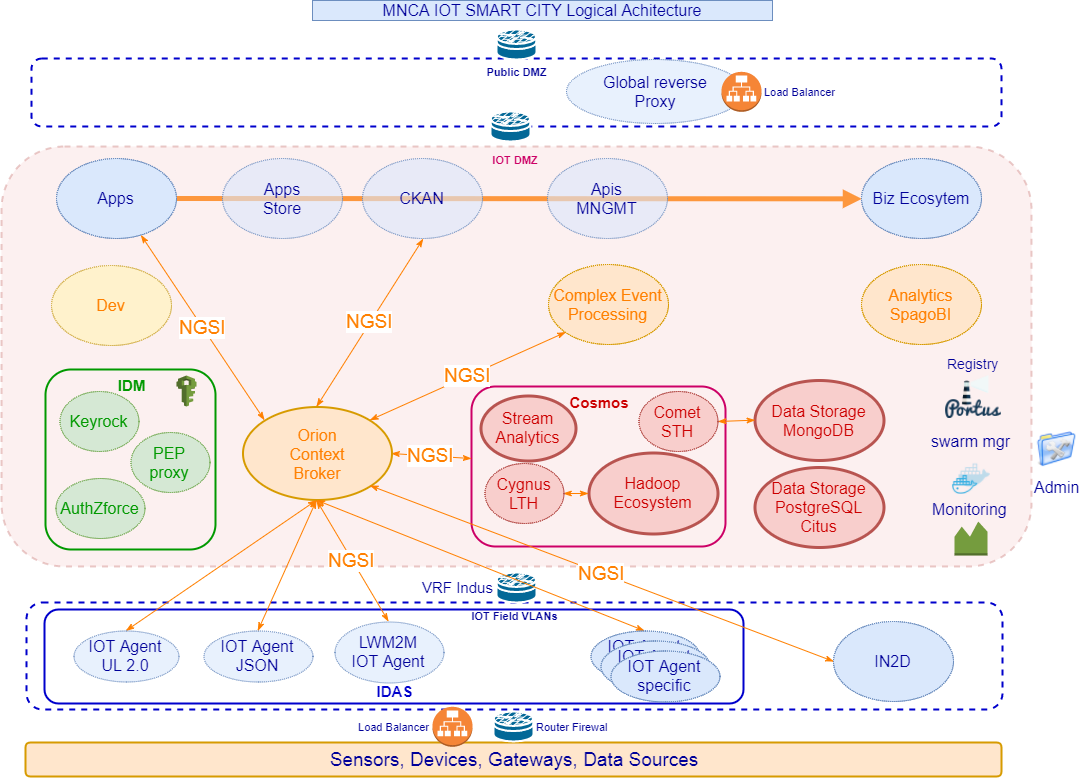


Figure 4: MNCA IOT Smart City Platform logical architecture

* Not all the relations between components have been represented in the above schema
* The central component that provides the main “super data bus” is the Orion Context Broker, this is a Fiware General Enabler (GE)
* As any interaction with this component is done using NGSI REST APIs, this is the main communication stream in the platform, that is represented on the above figure.
* As well the transversal arrow to Biz ecosystem GE, represent the link of each component to it for platform assets catalog management and monetization.
* Are not represented the relations to the identity manager (IDM GE) component, which are generally used to authorize access to the component through a proxy to identity manager.
* The aim with the IDM component, is to try to offer a centralized SSO management over the whole platform, allowing the central control of access authorization to platform components.
* The data storage component is not a Fiware component, this should be the SQL data tank of any Fiware module using SQL database, in case it’s impossible to change (a lot of Fiware modules rely on MySQL database) to PostgreSQL, we can use MariaDB.
* The general idea with the data storage components in the representation is to emphasis the fact that all the databases used by Fiware modules should be centralized in some clusters based on needed database server, which is true for SQL database and NoSQL database, so that relation links have not been represented on the above schema
* Inside the DEV component on the above figure are the Paas and the tools needed to develop applications that will use the Fiware ecosystem, this encompass development tools but also QA tools for testing and validation purpose, which can have specific needs in term of access to data. Most probably for development and QA, it will be required to deploy some Fiware components or even a complete platform for staging.
* A global reverse proxy and load balancer (F5 BigIP) will be the main entry point to the smart city platform.

### 2.2.1 Overall Architectural Considerations

*The* ***Overall Architectural Considerations*** *section defines how additional technical requirements have been addressed by the architecture. items in this section include:*

* *Deployment strategy*
* *Security Strategy*
* *Availability requirements*
* *Performance requirements*
* *Accessibility*
* *Database management*
* *Transaction volumes*
* *Concurrent users & devices*
* *Data import and export*
* *Disaster recovery*
* *GDPR*

#### Deployment Strategy

As stated previously, the MNCA Smart City platform will be deployed using Docker containers in a global swarm (group of Docker engines).

In this first step Docker engines will be deployed on Virtual machines dispatched on the 3 data centers (when they will be available).

The different modules will be grouped in services and stacks (Docker concepts).

Only Database servers, will be deployed in clusters, at disposal for use by other components of the platform.



#### Security Strategy

Security is achieved through a global identity and access rights management component the Fiware Identity Management GE, providing SSO and secure access to other components of the platform, according to requester authorizations.

#### Availability requirements

All the components used in the platform will be deployed in a way providing high availability.

The services and the associated databases should ideally be deployed on the 3 data centers,

The third data center remaining off-line most of time, should host replicas of the databases, updated in real-time.

The use of Docker provides an easy way to deploy highly available services, by deploying several containers on several nodes of a swarm, using docker compose files or docker stack files.

#### Performance requirements

Any of the components will be scalable by adding some instance of containers to scale-up the service.

Through the use of Docker it is very easy to achieve by changing services configuration on the fly.

#### Accessibility

Nothing specific is included in Fiware for accessibility, this item is to be considered at application UI level, most probably using accessibility features from operating systems or internet browsers that host the client application.

#### Database management

Different kind of databases are used among the Fiware components:

PostgreSQL, MySQL, MongoDB, and an Hadoop cluster.

To simplify the maintenance:

PostgreSQL should replace MySQL in each component where it’s possible, if it’s not possible MariaDB should replace MySQL without change.

To rationalize the architecture, each kind of database service will be deployed once in the platform, shared by the client components.

Each of the database service will be based on a cluster:

* This is native architecture for MongoDB
* PostgreSQL databases will be based on a Citus cluster
* MySQL databases will be based on a Galera cluster

May be thinking to master data management at the occasion of this project is an opportunity to consider

In particular to reach GDPR conformity more easily, by using appropriate tools to manage data and the access rights.

#### Transaction volumes

No specific requirement, best effort will be observed, but as the database clusters will be easily scalable, the transaction volume increase can be anticipated.

For that the monitoring system must have detailed history about transaction activity to be compared to processing/storage/network activity of the system, in order to be able to analyze the need of adding a node to the cluster, or just another container.

#### Concurrent user & devices

No specific requirement.

The scalability of the platform allows to virtually support any numbers of concurrent users and devices, providing the provisioning of enough computing nodes and bare metal servers to absorb the load.

#### Data import and export

Data existing in the current data warehouse will be imported into the new platform, the main concern remains the current data model adaptation to existing [Fiware data models](https://www.fiware.org/data-models/) and eventually propose amendments when needed.

This is currently under study, in order to be able to propose a table of correspondence between the existing data source attributes and the attributes defined in the schema for the destination data object (an NGSI entity), that, if possible, match an existing Fiware data model.

In case new attributes need to be added to a Fiware proposed model, or new data model, the proposal should be sent to Fiware for validation, respecting the given guidelines on [How To Contribute](https://github.com/fiware/dataModels#how-to-contribute).

#### Disaster recovery

The 3 data centers should be involved in the smart city platform then in case of serious problem in the main and secondary data center, the third DC, more protected from disaster like flood, can take over, and keep the platform online.

The databases used within the platform, must be replicated in real time on the third data center, to be able to use it in the shortest time possible.

#### GDPR

Observing General Data Protection Regulation will be mandatory on May 25th 2018, it’s a recent European directive defining new rules for personal data management.

Here are the major changes that are mentioned in this new legislation:

* **Consent:** Consent of personal data must be freely given, specific, informed and unambiguous. Consent is not freely given if a person is unable to freely refuse consent without detriment.
* **Accountability and privacy by default:** The GDPR has placed great emphasis on the accountability for **data controllers** to demonstrate data compliance. They will be required to maintain certain documentation, conduct impact assessment reports for riskier processing and employ data protection practices by default, such as data minimisation.
* **Notification of a data breach: Data controllers** must notify the Data Protection Authorities as quickly as possible, where applicable within 72 hours of the data breach discovery.
* **Sanctions:** This new legislation allows the Data Protection Authorities to impose higher fines – up to 4% of annual worldwide turnover. The maximum fines can be applied for discrepancies related to international data transfers or breach of processing principles, such as conditions for consent. Other violations can be fined up to 2% of annual worldwide turnover.
* **Role of data processors: Data processors** will now have direct obligations to implement technical and organisation measures to ensure data protection, this could include appointing a **Data Protection Officer** if needed.
* **One stop shop:** This legislation will be applicable in all EU states without the need of implementing national legislation. Having a single set of rules will benefit businesses as they will not need to comply with multiple authorities, streamlining the process and saving an estimate of €2.3 billion a year.
* **Removal of notification requirement: T**he requirement of notifying or seeking approval from a Data Protection Authority is going to be removed in many circumstances. This decision is made to save funds and time. Instead of notification the new directive requires **data controllers** to put in place appropriate practices for large scale processing in the form of new technology.
* **Right to be forgotten:** Persons will be able to require their data to be deleted when there is no legitimate reason for an organization to retain it. Following, the organisation must also take appropriate steps to inform any third party that might have any links or copies of the data and request them to delete it.
* **Expanded territorial reach:** Companies that are based outside of the EU, but targeting customers that are in the EU will be subject to the GDPR which is not the case now. (Not Applicable for the project).

Data Protection Act identifies Data controllers and Data Processors as separate jobs:

<https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf>

The new GDPR rules described above will have to be applied mostly in the applications involving the use of personal data (in particular data from citizens).

However, as the platform will be recipient of many different kind of data, it could be hard to embrace the complexity of the data sets possible entanglement, some data can be related to citizens, because coming from objects/sensors at home, even weared, or simply published through applications.

Then to have a Data Protection office is worth to consider (if not already acted), but this is beyond the scope of this document.

The multitenant nature of the Fiware platform help a lot to data protection & privacy by dividing into independent services with secure and controlled (authorized and authenticated) access to data-sets, provided by global security IDM component.

However, in the case of cross usage of multiple history datasets like in some data-science cases, data must be anonymized and minimized, before being delivered for analysis, this is to consider either at data acquisition step and data consuming step.

## System Architecture Component Definitions

### Security Component IDM GE

This component is the Fiware GE responsible for Fiware platform global user identity & access rights management

It is composed of 3 elements:

* the Identity Manager GE, in fiware catalog: [Keyrock](https://catalogue.fiware.org/enablers/identity-management-keyrock)
* the Access Control GE, in fiware catalog: [AuthZForce](https://catalogue.fiware.org/enablers/authorization-pdp-authzforce)
* GE module to add security to backend applications, in fiware catalog: [PEP Proxy](https://catalogue.fiware.org/enablers/pep-proxy-wilma)

|  |  |
| --- | --- |
| **Architecture Component** | **Component Elements** |
| Database Server | changed to Postgresql/Citus instead of MySQL |
| Applications | Keyrock (API backend + front-end: Horizon Django based application)  AuthZforce  PEP Proxy |



### Orion Context Broker Component

This component is central to the Fiware platform: this is the data exchange bus of the platform.

The reference implementation of the Publish/Subscribe Context Broker GE.

Orion Context Broker allows to manage the entire lifecycle of context information including updates, queries, registrations and subscriptions.

It is an [NGSIv2](http://fiware.github.io/context.Orion/api/v2/stable/) server implementation to manage context information and its availability.

on Fiware catalog: [Orion Context Broker](https://catalogue.fiware.org/enablers/publishsubscribe-context-broker-orion-context-broker)

|  |  |
| --- | --- |
| **Architecture Component** | **Component Elements** |
| Database Server | MongoDB |
| Applications | Orion context broker |

### MongoDB Component

This component is the [MongoDB](https://www.mongodb.com/) NoSQL database cluster global to the platform.

Several Fiware components use MongoDB to persist data, among them: Orion, IDAS, Comet STH

### Citus/PostgreSQL Cluster Component

This component is the cluster of [PostgreSQL](https://www.postgresql.org/) database servers of the Fiware platform.

The component is based on [Citus](https://www.citusdata.com/product/community), an open source clustering solution for PostgreSQL.

PostgreSQL is used by several components in the platform: such as CKAN, and those that will be changed from MySQL to PostgreSQL like Keyrock, Biz Eco System

### Galera/MySQL Cluster Component

This component is the cluster of MySQL database servers of the Fiware platform.

To provide high availability and scalability the component will be based on a clustering solution proposed by MariaDB: [Galera cluster](http://galeracluster.com/products/)

### Cosmos Big Data Component

This component is the Big Data and data history GE of the Fiware platform.

it’s composed of many modules:

Cygnus

Comet STH for Short Term History

Hadoop ecosystem

### Knowage Analytics Component

This component is for business intelligence, Fiware have originally chosen SpagoBI as the reference platform for this Analytics GE.

In the Fiware catalog is proposed the evolution of SpagoBI to a more integrated suite with all modules included: [Knowage](https://catalogue.fiware.org/enablers/data-visualization-knowage)

This GE provides the following features:

* BD (big data), to analyse data stored on big data clusters or NoSQL databases
* SI (smart intelligence), the usual business intelligence on structured data, but more oriented to self-service capabilities and agile prototyping
* ER (enterprise reporting), to produce and distribute static reports
* LI (location intelligence), to relate business data with spatial or geographical information
* PM (performance management), to manage KPIs and organize scorecards
* PA (predictive analysis), for more advanced analyses
* EI (embedded intelligence), to link Knowage with external solutions provided by the customer or third parties.

### CKAN Open Data Component

This component is the chosen GE to manage Open Data

CKAN GE at Fiware: <https://catalogue.fiware.org/enablers/ckan>

Fiware Docker installation: <https://github.com/okfn/docker-fiware-ckan>

Official installation guide : <http://docs.ckan.org/en/ckan-2.3.5/maintaining/installing/install-using-docker.html>

The CKAN GE provides the following features:

* Complete catalog system with easy to use web interface and a powerful API
* Strong integration with third-party CMS’s like **Drupal** and WordPress
* Data visualization and analytics
* Workflow support lets departments or groups manage their own data publishing
* Fine-grained access control
* Integrated data storage and full data API
* Federated structure: easily set up new instances with common search

|  |  |
| --- | --- |
| **Architecture Component** | **Component Elements** |
| Database Server | Postgresql/Citus |
| Applications | Api and WEB UI  CMS integration (WP, Drupal) |

### IDAS Component

The IDAS component is an implementation of the Backend Device Management GE.

It provides software for IOT use cases, to manage communication between devices/gateways and the data context broker.

On Fiware Catalog: [IDAS](https://catalogue.fiware.org/enablers/backend-device-management-idas)

|  |  |
| --- | --- |
| **Architecture Component** | **Component Elements** |
| Database Server | MongoDB |
| Applications | UL2.0 IOT Agent  JSON IOT Agent  IOT Agent library to develop others agents |

### CEP Component

The CEP component is the Complex Event Processing GE from the Fiware platform.

In Fiware catalog is proposed an implementation from IBM of the CEP module: [PROTON](https://catalogue.fiware.org/enablers/complex-event-processing-cep-proactive-technology-online)

It is a scalable integrated platform to support the development, deployment, and maintenance of event-driven applications.

Telefonica propose also an implementation of the CEP GE: [Perseo](http://fiware-iot-stack.readthedocs.io/en/latest/cep/), as the CEP GE of their IOT stack

As well as Orange which propose [Cepheus](https://catalogue.fiware.org/enablers/iot-data-edge-consolidation-ge-cepheus)

It’s composed of a light NGSI broker and a CEP which features a dedicated REST management API to configure real time analysis on NGSI events.

The CEP from Telefonica **Perseo** has been chosen for the MNCA platform

|  |  |
| --- | --- |
| **Architecture Component** | **Component Elements** |
| Database Server | MongoDB |
| Applications | Perseo core engine (rules processing)  Perseo Front-end (Rules definition & storage) |

### Application Mashup Components

Wirecloud is the Fiware GE to build Rich Internet Applications (RIA), using semantic technologies to offer a next-generation end-user centered web application mashup platform.

Fiware Catalog: [Wirecloud](https://catalogue.fiware.org/enablers/application-mashup-wirecloud)

|  |  |
| --- | --- |
| **Architecture Component** | **Component Elements** |
| Database Server | Postgresql/Citus |
| Applications | Web application  back-end server |

web application mashup platform aimed at allowing end users without programming skills to easily create web applications and dashboards/cockpits.

Alternatively a small javascript library like [Freeboard](https://github.com/Freeboard/freeboard) can be used to visualize data coming from NGSI context broker: [news on Fiware](https://www.fiware.org/2015/07/13/fiware-orion-data-source-now-available-for-freeboard/)

### Biz Ecosystem Component

The Business API Ecosystem exposes its complete functionality through TM Forum standard APIs; concretely,

it includes the following key features:

* Support for the management of catalogs, products, and offering
* Support for rich pricing models, including recurring payments, pay-per-use, etc.
* Support for accounting callbacks
* Support for billing and charging
* Integrated support for PayPal, including customer charges and seller payments
* Support for revenue sharing, including models with multiple stakeholders involved

Link to Fiware catalog: [Biz Api Ecosystem](https://catalogue.fiware.org/enablers/business-api-ecosystem-biz-ecosystem-ri)

Link to the documentation: <http://business-api-ecosystem.readthedocs.io/en/latest/>

|  |  |
| --- | --- |
| **Architecture Component** | **Component Elements** |
| Database Server | Postgresql/Citus (change from MySQL) |
| Applications | Web application  back-end server |

TM Forum APIs and RSS requirements

* Java 8
* Glassfish 4.1
* MySQL 5.5 => replace with PostgreSQL/Citus or use Galera Cluster ?

Charging Backend requirements

* Python 2.7
* MongoDB
* wkhtmltopdf

Logic Proxy requirements

* NodeJS 4.5.0+ (Including NPM)

### Development Components

Fiware propose to use fusionforge as the set of tools for development

Now with the advent of Docker, Eclipse have evolved towards the paradigm and propose Eclipse Che

If for many applications Wirecloud component is a good solution, for more complex or even mobile application it is not adapted, so that Eclipse Che is a good alternative.

### Monitoring Components

Portainer for realtime management

Centreon is already in use at MNCA, containers should be instrumented with needed NRPE modules to monitor services and nodes in the platform from the Centreon, an additional Centreon service should be added in the platform.

### Docker Images Management Component

As MNCA needs to manage its own Docker images, [Portus](http://port.us.org/) has been chosen as the component for that task.

It’s an [open source software originated from Suse](https://github.com/SUSE/Portus), written in Ruby, providing it’s own security acces layer

### Docker Swarm Management Component

Swarm manager is the orchestrator of the services based on the components of the platform.

It’s part of Docker software suite.

# Section 3 SYSTEM ARCHITECTURE DESIGN

*The* ***System Architecture Design*** *section provides detailed descriptions of each product implementing architecture components, and explains the rationale for product selection.*

*For each* ***System Architecture Component*** *(identified in Section 2.3 above), this section describes: specific* ***Component Functions****, requirements and other* ***Technical Considerations*** *that were used in the decision-making process, as well as any specific* ***Products*** *selected to implement this component. The* ***Selection Rationale*** *identifies any other products that may have been considered, and provides rationale for the decision.* ***Architecture Risks*** *identifies any potential risks associated with the architecture element.*

## 3.1 Security Component IDM GE

### Component Functions

Manage globally the security for the Fiware platform, in terms of identity and access authorization to services and data.

The Keyrock module provides identity management Keystone back-end, the integrated web UI is provided through Horizon front-end, which allows user accounts management.

The AuthZforce component provides roles and access rights management

The PEP Proxy components provides Keyrock security to others back’end of the platform such as Orion context broker

### Technical Considerations

This is the components proposed in Fiware catalog,

It’s based on **Keystone**, the IDM component of OpenStack cloud software suite.

it use the standard OAuth2 protocol

it can connect with an LDAP if needed

### Selected Product(s)

OpenStack **Keystone** provides authentication, authorization and service discovery mechanisms via HTTP primarily for use by projects in the OpenStack family. It is most commonly deployed as an HTTP interface to existing identity systems, such as LDAP.

### Selection Rationale

### Architecture Risks

## Orion Context Broker Component

### Component Functions

### Technical Considerations

### Selected Product(s)

There’s another implementation of an NGSI context broker originated from Orange:

### Selection Rationale

### Architecture Risks

This component is central to the platform, because it’s the dorsal of the architecture

It can become a bottleneck in case of high traffic, so a particular attention is needed on response time, through specific monitoring

## MongoDB Component

### Component Functions

MongoDB is a NOSQL document database, natively scalable

### Technical Considerations

### Selected Product(s)

### Selection Rationale

### Architecture Risks

## Citus/PostgreSQL cluster Component

### Component Functions

### Technical Considerations

### Selected Product(s)

### Selection Rationale

### Architecture Risks

## Galera/MySQL cluster Component

### Component Functions

### Technical Considerations

### Selected Product(s)

### Selection Rationale

### Architecture Risks

## Cosmos Big Data Component

### Component Functions

### Technical Considerations

### Selected Product(s)

### Selection Rationale

### Architecture Risks

## Knowage Analytics Component

### Component Functions

### Technical Considerations

### Selected Product(s)

### Selection Rationale

### Architecture Risks

## CKAN Open Data Component

### Component Functions

### Technical Considerations

### Selected Product(s)

### Selection Rationale

### Architecture Risks

## IDAS Component

### Component Functions

### Technical Considerations

### Selected Product(s)

### Selection Rationale

### Architecture Risks

## CEP Component

### Component Functions

### Technical Considerations

### Selected Product(s)

### Selection Rationale

### Architecture Risks

## Application Mashup Component

### Component Functions

### Technical Considerations

### Selected Product(s)

### Selection Rationale

### Architecture Risks

## Biz Ecosystem Component

### Component Functions

### Technical Considerations

### Selected Product(s)

### Selection Rationale

### Architecture Risks

## Development Components

### Component Functions

### Technical Considerations

### Selected Product(s)

### Selection Rationale

### Architecture Risks

## Monitoring Components

### Component Functions

### Technical Considerations

### Selected Product(s)

### Selection Rationale

### Architecture Risks

## Docker Images Management Component

### Component Functions

### Technical Considerations

### Selected Product(s)

### Selection Rationale

### Architecture Risks

## Docker Swarm manager Component

### Component Functions

### Technical Considerations

### Selected Product(s)

### Selection Rationale

### Architecture Risks

# Section 4 System Construction Environment

*The* ***System Construction Environment*** *section details the various environments necessary to enable system construction and testing.*

## Development Environment

### Developer Workstation Configuration

### Supporting Development Infrastructure Configuration

## QA Environment

### QA Workstation Configuration

### Supporting QA Infrastructure Configuration

## Acceptance Environment

*For each environment necessary for system construction (****Development, QA*** *and* ***Acceptance****), provide detailed specifications for the* ***Workstation*** *and* ***Supporting Infrastructure*** *that will be used (including hardware, network and operating system requirements, all necessary installed packages and tools, and needed directory structures**that will be utilized to store all construction components).*

### Acceptance Workstation Configuration

### Supporting Acceptance Infrastructure Configuration